U.S. Marine Corps Forces, Pacific
Force Protection

Newsletter

4th Quarter CY21

Mission

To ensure that U.S. Marine Corps Forces operating within or transiting through, the U.S. Indo-Pacific Command (USINDOPACOM) Area of Responsibility (AOR) are prepared to survive, respond to, and recover from enemy threats and natural hazards, in order to ensure freedom of action and continuity of operations.

From the Branch Head:

This newsletter contains important updates from across the Force Protection community. The Counter-Insider Threat page outlines key information defining insider threats, detection, and mitigation. This information is vital to ensure individuals exhibiting concerning behavior are provided the assistance they need with the goal of preventing an insider threat incident from occurring in the first place.

Per DoDI 6055.17 Ch3, all DoD military, civilian, and contract personnel must be registered in an Electronic Mass Notification System (EMNS). AtHoc is the EMNS used by both Marine Corps Base Hawaii, and Headquarters MARFORPAC to provide personnel and family members assigned to these commands with electronic notification of impending threats and/or associated actions (e.g. destructive weather event, active shooter, Crisis Action Team recall, etc.). Recent tests of the MARFORPAC EMNS have resulted in poor results. The Emergency Management page contains user information to enroll and update of their information within the AtHoc system. Please contact the Force Protection Branch for any assistance regarding AtHoc system administration.

Updates to the continuous evaluation/process for those DoD personnel who hold a security clearance are outlined on the Personnel Security page, along with specific information from each of the functions/programs from the joint protection function that comprise the Force Protection program.

Lastly, one of our own, Mr. Kevin Keenan "K2" was recognized by DC PP&O (PL) Foreign Disclosure Section, as the Foreign Disclosure Officer (FDO) of the Quarter for 4Q FY21 for his hard work and dedication in supporting the USMC Foreign Disclosure program. BZ to K2!

- *Brian J. Whalen*

The MARFORPAC Force Protection Newsletter is open to input from across the MARFORPAC staff, and the USMC Force Protection/Installation Protection community. Please email topic ideas, articles, or questions to: marforpac.forcepro@usmc.mil

Table of Contents

Community Updates

MCDP-X, Marine Corps Protection
- New Publication
- **2d O6 level review completed 17 Dec 2021**
- OPR, DC PP&O, Security Division (PS)

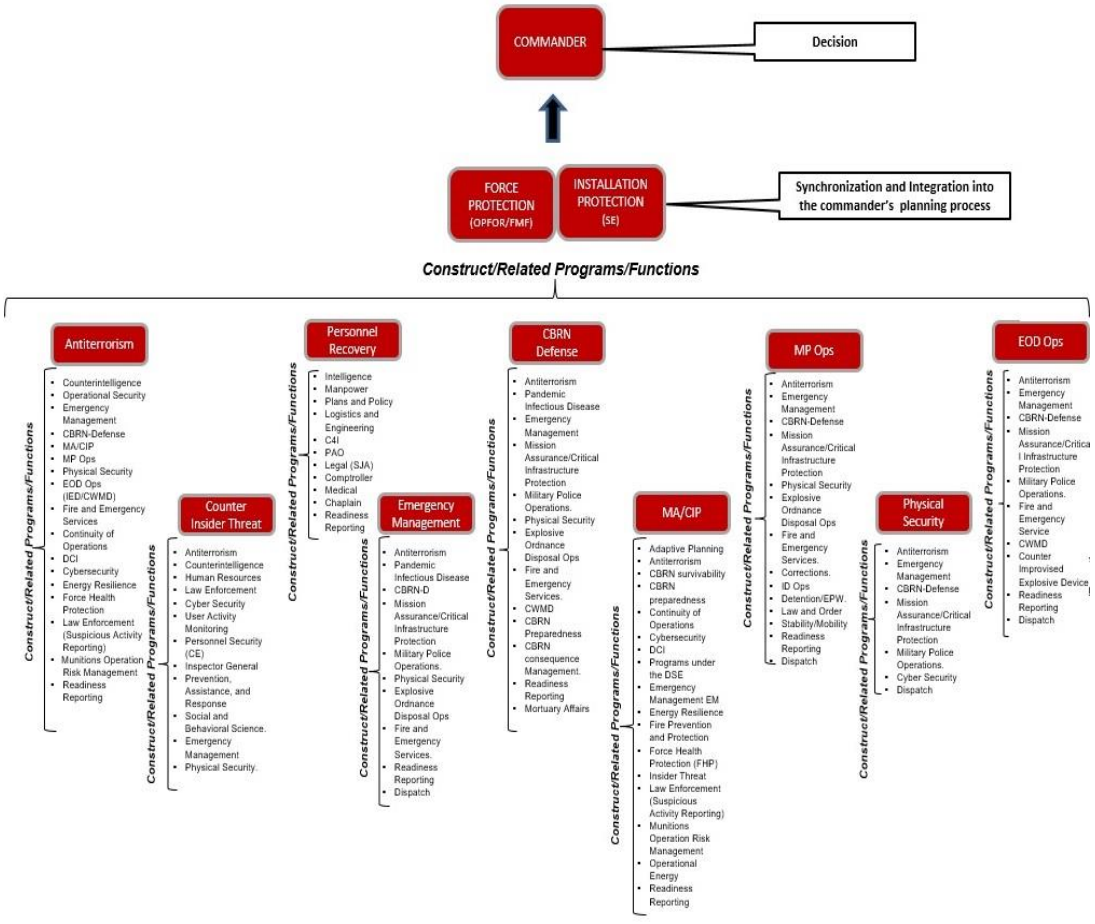
MCWP 10-10, Marine Corps Protection
- New Publication.
- In Draft (OPR, USMC Protection Council)

Marine Corps Protection Policy
- New Publication
- In Draft (OPR, USMC Protection Council)

MARFORPAC Force Protection Policy
- New Publication
- In Draft (OPR, MFP Force Protection)

MCO 3440.0, Marine Corps Emergency Management Program
- Cancels and replaces MCO 3440.9
- **Sep 2021, Completed O6/GS15 level review**

MARPFORPAC CBRND Program
- New Order
- **Currently out for signature**



Joint Intermediate Force Capabilities

Pre-Emplaced Electric Vehicle Stopper

What is it?
The Pre-Emplaced Electric Vehicle Stopper (PEVS) is a compact counter-materiel intermediate force capability that can stop a targeted vehicle by injecting high-powered electrical impulses into its engine. PEVS is portable, can be operated remotely, and engage hundreds of targets before requiring any significant maintenance.

How does it work?
When armed, two spring-loaded electrodes extend upward to deliver a short-duration electrical pulse as they contact the undercarriage of a passing car, truck, or van. The charge causes its electronics to malfunction temporarily, stopping the vehicle. The driver can restart the engine and continue to his/her destination after security personnel determine that no threat was present.

Operational impact:
PEVS complements an installation's robust entry control point (ECP) measures by providing forces with additional decision time and space to validate that a perceived hostile intent/act is, in fact, hostile. Users can engage large and small vehicles at safer standoff ranges without harming passengers or personnel, mitigating potential vehicle-borne threats. This capability supports the full range of military operations inherent in the National Defense Strategy's framework and across the competition continuum.

PEVS stops vehicles at significant stand-off ranges, reducing risk to personnel from vehicle-borne improvised explosive device blast effects

The system's high-powered pulse causes the targeted vehicle's electronics to malfunction temporarily without harming its occupants.

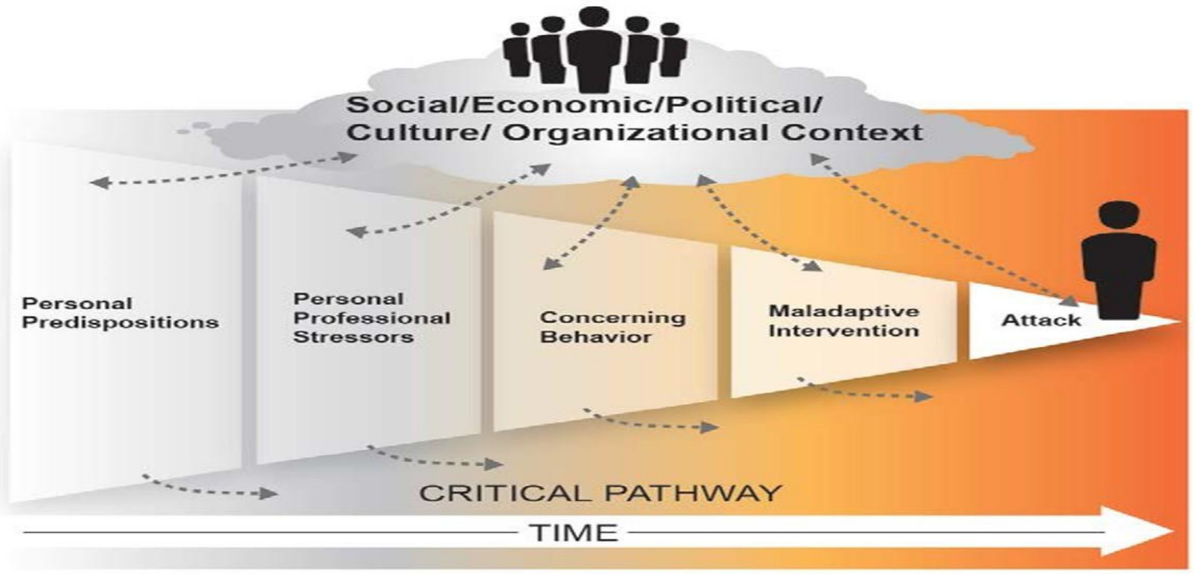
Counter Insider Threat

What is an Insider Threat?
Any person who has or once had authorized access to any US government resource to include personnel, facilities, information, equipment, networks, or systems…

AND

…will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat includes potential espionage, violent acts against the Government or the Nation including terrorism, unauthorized disclosure of national security information, or the loss or degradation of departmental resources or capabilities.

Insider Threat Detection
Detection of potentially malicious behavior involves authorized insider threat personnel gathering information from many sources, and analyzing that information for clues or behaviors of concern. A single indicator may say little, however, if taken together with other indicators, a pattern of concerning behaviors may arise. It is important to consider relevant information from multiple sources to determine if an individual's behavior deserves closer scrutiny, or whether a matter should be formally brought to the attention of the chain of command, an investigative or administrative entity.



Insider Threat Assistance
Concerning behaviors can be interrupted or stopped completely by successful intervention from a supervisor, community service program or health care professional depending on the situation. It is also possible that the individual has no malicious intent, but is in need of help. The **first step** in successful mitigation of insider threats is to get them the help that they need.

Antiterrorism Operations

Irregular Warfare in the Littorals

Irregular Warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will.

Two areas of the Littorals:

- The seaward portion is the area from the open ocean to the shore that must be controlled to support operations ashore.
- The landward portion is the area inland from the shore that can be supported and defended directly from the sea.

Threat:

Peer/Near Peer adversaries are frequent practitioners of irregular warfare which can include:

- Unmanned Underwater Vehicles (UUV's)
- Grey zone activities (Territorial encroachment, Cyber, proxy forces)
- Sea Mines
- Military occupation of atolls

Terrorist/Non-State Actors may employ:

- Improvised Explosive Device -USS Cole
- Kidnapping - Abu Sayyaf boat raid on Palawan 20 people abducted from the resort
- Amphibious Raid - Pakistan to Mumbai
- Semi- Submersible – Drug Cartels

Piracy (illegal act of violence or depredation that is committed for private ends on the high seas or outside the territorial control of any state) occurs in the below locations within the INDOPACOM AO:

- Straits of Malacca
- The Bay of Bengal

Mitigation Measures:

- Blue/Green integration
- Intelligence
- Ship riders/Topside rovers
- Q- routes
- SIGMAN
- OPSEC
- Hardening (fighting positions /landing crafts
- OP/LP's
- MILDEC

Personnel Recovery

Recovery is an implied task for all exercises and operations. There are three different types of recovery, Immediate Recovery, Deliberate Recovery, and External Supported Recovery.

Immediate Recovery occurs as soon as it is recognized there is an accountability issue with Marines and/or others under your command. This can occur due to daily personnel reporting, missed checkpoints, overdue aircraft or vehicles or during consolidation. The best time to perform a recovery mission is as soon as a missing person is identified.

Deliberate Recovery is the direct use of an identified unit or force, such as a TRAP Team. It can include integrated capabilities such as air, ground and maritime forces. The Personnel Recovery Coordination Cell (PRCC) are responsible to conduct multi echelon coordination and de-conflicting internal and external forces. This continues until the isolated personnel are recovered successfully regardless of recovery capabilities.

External Supported Recovery is the sum of coordination and support provided by any external forces to the Marine Corps. It is a requirement for components of a joint force to plan for and support PR operations.

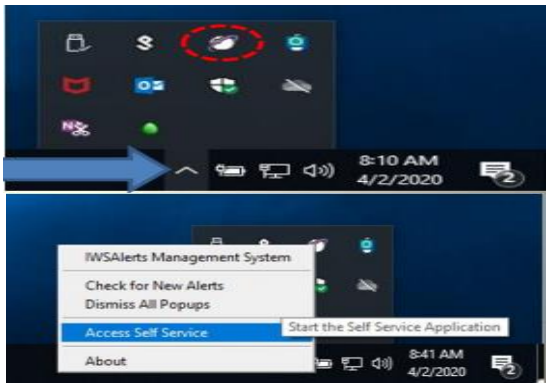
Isolated personnel have the responsibility to facilitate their own recovery to the maximum extent possible. All elements of a MAGTF possess the ability to participate and or support the recovery of isolated personnel through TRAP operations.

Emergency Management

AtHoc

Per DoDI 6055.17 Ch3, all DoD military, civilian, and contract personnel must be registered in an Electronic Mass Notification System (EMNS). AtHoc is the **electronic Mass Notification System (eMNS)** used by both Marine Corps Base Hawaii, and Headquarters MARFORPAC to provide personnel and family members assigned to these commands with electronic notification of impending threats and/or associated actions (e.g. Destructive weather event, Active Shooter, Crisis Action Team Recall, etc.). The MARFORPAC Force Protection Branch provides policy for eMNS, and serves as the system administrators for use of the AtHoc system by HQTRS MARFORPAC personnel.

Update Contact user information from your NIPR computer:
1) Select the up arrow at the bottom right of your desk top.
2) Select the purple globe.
3) Select Access Self Service.
4) Select My Profile at the top left.
5) Select Edit at the top left.
6) You can now update your personal



Responding to Alerts:

Desktop (NIPR computer/email):
Desktop alerts will display as popup windows. After reading the alert, click the Acknowledge and Close button. Clicking the Acknowledge and Close button sends a response to the AtHoc system, which tracks, compiles, and reports all recipient responses.

Mobile Phone Text:
Users who get receive an alert via text on their mobile phone will be able to respond to the text alert with the specific response options that the AtHoc Administrator created. Users can do this in the alert message they receive. MARFORPAC users will press "1" on the phone keypad, or type "1" in the text box and press send to acknowledge.

Land-Line Phone:
Users who get receive voice alerts via their land-line phone will be able to respond by pressing "1" on the phone keypad, to acknowledge, or verbally stating acknowledgement when prompted.

Personal Email on Home Computer and/or Smart Phone:
Users who get receive an email alert on their home computer and/or smart phone will be able to respond to the email alert by typing 1 in the response block and hitting send.

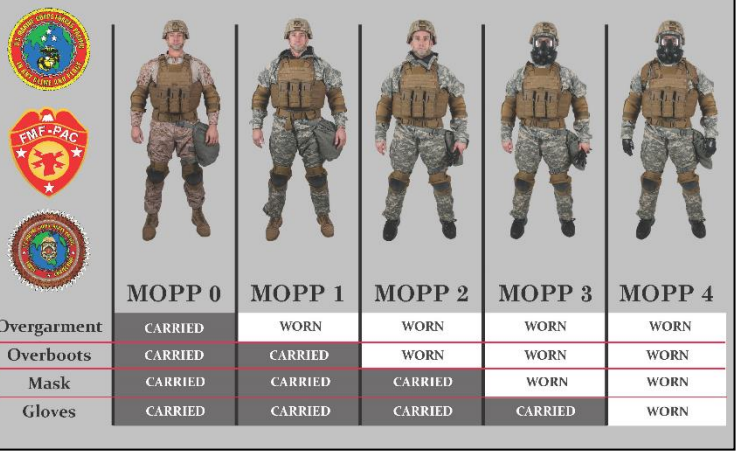
CBRN Defense (Operations)

Contamination Mitigation is the planning and actions taken to prepare for, respond to, and recover from contamination associated with all CBRN threats and hazards to continue military operations. Unit SOPs shall prescribe contamination mitigation procedures in an effort to minimize the exposure and potentially minimize the thermal burden associated with the effect of augmented Mission Orientated Protective Posture durations. The below graphics display proper MOPP levels in and out of combat gear.

Mission Oriented Protective Posture (MOPP) : Without Personal Protective Equipment

	MOPP 0	MOPP 1	MOPP 2	MOPP 3	MOPP 4
Overgarment	CARRIED	WORN	WORN	WORN	WORN
Overboots	CARRIED	CARRIED	WORN	WORN	WORN
Mask	CARRIED	CARRIED	CARRIED	WORN	WORN
Gloves	CARRIED	CARRIED	CARRIED	CARRIED	WORN

Mission Oriented Protective Posture (MOPP) : With Personal Protective Equipment



	MOPP 0	MOPP 1	MOPP 2	MOPP 3	MOPP 4
Overgarment	CARRIED	WORN	WORN	WORN	WORN
Overboots	CARRIED	CARRIED	WORN	WORN	WORN
Mask	CARRIED	CARRIED	CARRIED	WORN	WORN
Gloves	CARRIED	CARRIED	CARRIED	CARRIED	WORN

Support to CWMD

From 26-30 July 2021, 3d Mar Div G-3 CBRN platoon conducted exercise Habu Sentinel with 9th ESB EOD Marines and Air Force Emergency Managers aboard Camp Hansen Combat Town and Camp Lester abandoned hospital. This integration increases the joint collective response capabilities to respond to known and an unknown CBRN hazards on the battlefield, and to exploit and asses enemy CBRN capabilities. Ultimately, this exercise validates core METs and competencies for the division platoon in support to CWMD, CWMD proliferation, and regional OPLANs.

Training Objectives:

- 5711-SHD-100: Direct CBRN Individual Protective Measures
- 5711-SNS-1001: Locate the presence of a CBRN Hazard
- 5711-SNS-1002: Identify a CBRN Hazard
- 5711-SNS-1003: Confirm a CBRN Hazard
- 5711-SHP-1001: Perform CBRN Warning & Reporting
- 5711-SUS-1001: Perform CBRN decon
- 5711-SUS-1002: Direct CBRN operational decontamination
- 5711-TRG-1001: Conduct CBRN training
- 5711-TRG-1002: Conduct HazMat Ops
  5711-TRG-2002: Supervise CBRN training
- 5711-TRG-2003: Conduct HazMat Technician Operations
- 5711-TRG-2004: Manage HazMat Incident
- 5711-CCM-2001: Supervise support to CBRN CM Operations
- 5700-CCM-3001: Provide CBRN support for CM Operations
- 5700-CWMD-3001: Provide CBRN support to CWMD Operations
- 5700-SNS-3002: Support SSE Operations
- 5700-SUS-3001: Conduct decon operations

Critical Infrastructure Protection

The focus of the U.S. Marine Corps Forces, Pacific (MARFORPAC) Critical Infrastructure Protection (CIP) program is to identify, prioritize, and validate infrastructures, assets, and capabilities deemed critical to both joint and USMC operating forces ISO accomplishing their war-fighting missions.

MARFORPAC CIP concentrates on the development of plans to mitigate the effects of the potential loss or disruption of these critical infrastructures, assets, and capabilities. To maintain operational and tactical readiness, commanders and forces must understand the importance of their assets, perform continuous threat and vulnerability assessments of mission critical assets, successfully manage their dependencies and risk of loss or degradation, and plan for their continuity of operations (COOP).

Critical Infrastructure is a key component fed into operational planning for Critical Asset List (CAL) and Defended Asset List (DAL) development.

By executing the CIP Program to ensure operational readiness, MARFORPAC will identify, protect, and ensure the availability of those assets and infrastructures critical to the execution of its mission in support of Combatant Commanders (COCOMs) and missions assigned by HQMC. Coordinating through the chain of command, MARFORPAC will be prepared to interface with sector lead agencies that provide infrastructure services within its area of responsibility. MARFORPAC will also be prepared to coordinate closely with appropriate Federal, state, and local government agencies, and critical non-DOD service providers to support mission critical capabilities and requirements.

The goal of the MARFORPAC CIP program is to identify and recommend means to mitigate risk to critical Infrastructures, assets, and capabilities, or to accept prudent risk where necessary.

Military Police Operations

Military Police support from the supporting establishment

CMC's Force Design Comment for divestment of Law Enforcement Battalions (LEBn):
This capacity is excess to our current needs, which can be met by the remaining force with some adjustments in current operational practice.

While many of the tasks previously assigned to the LEBns will be picked up by other units, there are still capabilities which the FMF may require which are now resident only in the supporting establishment. Requests for these capabilities must be directed to MCICOM. The below capabilities maybe required for future exercises and operations.

Military Working Dog (MWD). MWD teams are no longer resident in the FMF. With the divestment of the LEBn, the only off-leash explosive detection capability in DoD (outside of SOCOM) was eliminated. Installation Provost Marshal Offices (PMO) maintain Patrol Explosive Detection Dogs and Patrol Drug Detection Dogs. Marine MWD teams currently support installation security as well as support US Secret Service Very Important Persons Protection Support Activity (VIPPSA).

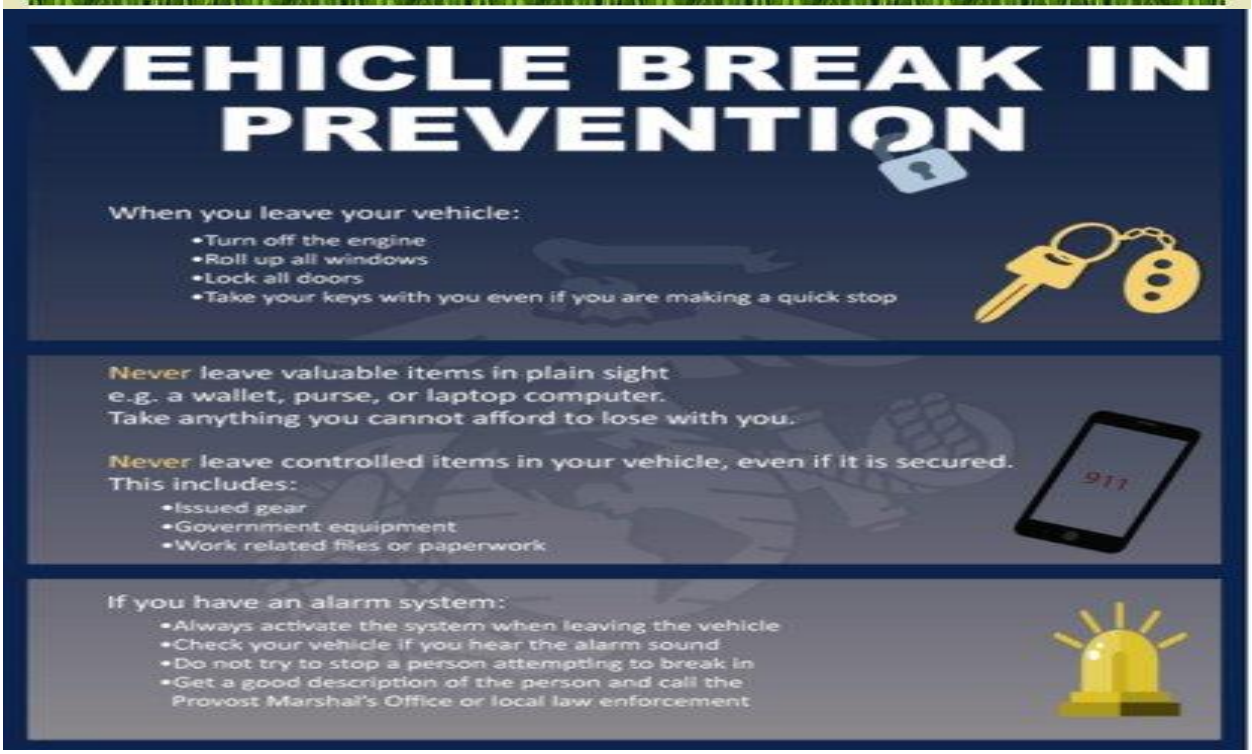
Criminal Investigators. The Criminal Investigators assigned to the LEBns had previously supported the FMF through augmenting NCIS force protection efforts, assisting commands with deployed criminal investigations and coordination with host nation law enforcement, as well as supporting Identity Operations.

Correctional Specialists. Corrections Marines can support and provide training for the execution of Detainee Operations. Detainee Operations training requirements for forces operating in the USINDOPACOM AOR are found in USINDOPACOM Instruction 2310.1.

Non-Lethal Weapons Instructors. Intermediate force capabilities give the commander additional options to counter adversaries attempting to exploit Rules of Engagement. Interservice Non-Lethal Individual Weapons Instructor Course (INIWIC) is the only recognized course to certify service members to provide instruction on Non-Lethal Weapons (NLW). Although any MOS can attend the course, the vast majority of Marine NLW Instructors are in the Military Police MOS. MARFORPAC receives INIWIC school quotas for I and III MEF units, which still have mission sets requiring intermediate force capabilities. Although the MEFs have the ability to maintain this capability, FMF units may be able to coordinate additional NLW instructors from installation PMOs.

Physical Security

Crime Prevention: No one is immune to crime. Ensuring to properly secure your homes and vehicles can prevent you from becoming a victim.



Explosive Ordnance Disposal

Humanitarian Mine Action (HMA) Three Year Plan

The goal of the HMA program is to save lives, relieve human suffering and other adverse effects of land mines, unexploded ordnance (UXO) and other Explosive Remnants of War (ERW) on noncombatants. The HMA program consist of the following courses: Physical Security Stockpile Management (PSSM), Basic EOD (EOD I), Intermediate EOD (EOD II), and Advanced EOD (EOD III).

HMA Three Year Plan				
Partner Nation Current Status	**FY2022**	**FY2023**	**FY2024**	**Endstate:**
Thailand: Gaps in advanced Demining and UXO/ERW tactics.	EOD I, II & III, Demining Tm Ops, Equipment Purchase CLEARPATH, EBINGER	EOD II & III, Demining Tm Ops, Equipment Purchase, Inst. Dev; HMA Virtual Trainer and Drone Pilot programs,	EOD II & III, Demining Tm Ops, Inst. Dev, Ops Center actions, Survey Management	Thailand free of landmines, UXO and ERW by 2025.
Palau: No organic Deminer/EOD capability. PN relies on NGO support.	EOD I & II, Blast Trauma Training, Equip Purchase, Instructor Development, EOD Level III	EOD I & II, Med Training, EOD Mission Planning, Instructor Development, Demining Tm Ops, Possible EOD III	TBD, pending country plan rewrite. Continued engagement anticipated	Palau National Safety Office demining capabilities are enhanced
Papua New Guinea: Very limited, if any, demining and PSSM capability.	EOD I & II, Blast Trauma Training, Equip Purchase	EOD I & II, Blast Trauma Training, Equip Purchase, Mission Planning, Instructor Development, Demining Tm Ops, Possible EOD III	EOD I & II, Blast Trauma Training, Equip Purchase, Mission Planning, Instructor Development, Demining Team Ops, Possible EOD III	UXO and ERW remediation capability improved
Timor Leste: Very limited, if any, demining and PSSM capability.	EOD I, Blast Trauma Training, Equip Purchase, Demining Tm Ops	EOD I, Blast Trauma Training, Equip Purchase, Demining Tm Ops	EOD I & II, Blast Trauma Training, Equip Purchase, Demining Tm Ops	Timor possess organic demining and UXO removal capabilities are enhanced
Cambodia: Gaps in advanced Demining and UXO/ERW tactics.	EOD I & II, Blast Trauma, Demining Tm Ops	Mentor, EOD I, Basic Med Training Potential USMC: Demining Tm Ops (South Prov.) PN Desire Under Asmt	Mentor, EOD I Refresh, EOD II, Basic Med Training, Demining Tm Ops (South Prov.)	VNMAC demining capabilities are enhanced

Personnel Security

DOD Now Continuously Monitoring Clearance Holders' Credit and Criminal Records

The long-awaited change to the background investigations process will flag concerning information for further investigation.

All Defense Department clearance holders are now officially part of a continuous vetting process to ensure they are entitled to keep their security clearances as their circumstances change.

As part of the broader Trusted Workforce 2.0 program—a joint effort between DOD, the intelligence community, the Office of Personnel Management, and the Office of Management and Budget—the Defense Counterintelligence and Security Agency, or DCSA, has been working to automate parts of the background investigations process. That work includes shifting from manually reviewing existing clearance holders every five to 10 years, to an ongoing process dubbed "continuous vetting."

The continuous vetting process includes automated checks on pertinent records such as financials and credit, arrests and citations by law enforcement, foreign travel, terrorism watch lists and internal investigations by other federal agencies. The program also looks at public social media posts and other online activity.

When potentially concerning information is discovered, the system is designed to flag those findings for adjudicators, who investigate further before making a determination. In the past, such issues would only be addressed during the reinvestigation period or if a serious concern was raised through formal channels.

Ultimately, in the full TW 2.0 framework, continuous vetting will fully replace periodic reinvestigations by employing a full suite of automated record checks through the National Background Investigation Services.

By that time, DCSA plans to roll out continuous vetting for all clearance holders, including those within the rest of the federal government and industry folk who maintain clearances to work on government contracts.

The program expects to be fully operational by Oct. 1, 2023.

Foreign Disclosure

If you have a requirement to release/disclose information to a foreign government or international organization, then the product requires review for disclosure/release.

FDO: Foreign Disclosure Officers will ensure a judicious decision is made considering the disclosure/release of the request, while providing clear and well-reasoned analysis, guidance, and recommendations.

FDR: Foreign Disclosure Representative may be appointed to assist the Command FDO in the processing and coordination of their branch / sections foreign disclosure requests and make recommendations to the FDO.

Training: FDO's and FDR's must complete mandatory training as prescribed by DC PP&O (PL) and their local command policies as applicable.

In-Person: HQMC FD offers an information-packed FDO/FDR course, delivered over two days in person / three days virtually and includes a comprehensive, hands-on capstone activity that prepares new Foreign Disclosure Officers and Foreign Disclosure Representatives with the resources to be successful in safeguarding our National Security through a rigorous review process. Next Hawaii course is in Spring 2022.

Online: FDO's and FDR's can sign up by visiting the milSuite USMC Foreign Disclosure Training and Education site at:
https://www.milsuite.mil/university/usmcforeigndisclosure-class/register-for-fdo-courses/

Stopgap Training: For those who cannot attend the two days in person training due to restrictions, the stopgap training is still the best option. With the approval of the first FDO in your Chain of Command and PP&O PL, complete this curriculum for temporary appointment as a FDO/FDR. This is not meant to replace the Foreign Disclosure course but rather to fill the gap for those who need it until they can attend the HQMC course.

FDMS site (NIPR):
https://intelshare.intelink.gov/sites/marforpac/Sections/Security/Pages/FDMS_Dashboard.aspx

Contact Information

Organizational Email:
marforpac.forcepro@usmc.mil

Force Protection Officer/ Branch Head
Brian Whalen
808 477-8618
brian.j.whalen1@usmc.mil

Explosive Ordnance Disposal Officer/Deputy Branch Head
LtCol Dan Cusinato
808 477-8457
Daniel.cusinato@usmc.mil

CBRN-D SNCO/Branch Chief
MGySgt Kierre Campbell
808 477-8673
kierre.campbell@usmc.mil

Joint Intermediate Force Capabilities
Barclay Lewis
808 477-8920
barclay.lewis.ctr@usmc.mil

Antiterrorism Operations
Rob Norton
808 477-8718
robert.norton@usmc.mil

Personnel Recovery/ Foreign Disclosure Officer
Kevin Keenan
808 477-8923
kevin.keenan@usmc.mil

Physical Security
GySgt Keily Warren
808 477-1846
keily.warren@usmc.mil
marforpac.physec@usmc.mil

CBRN-Defense
CWO5 Brian Barksdale
808 477-5818
brian.barksdale@usmc.mil

MGySgt Kierre Campbell
808 477-8673
kierre.campbell@usmc.mil

Mike Bender
808 477-8380
michael.a.bender@usmc.mil

Critical Infrastructure Protection
Brian Nuss
808 477-8950
brian.nuss@usmc.mil

Military Police Officer/ Counter Insider Threat/ Emergency Management
LtCol Kris Knobel
808 477-8930
kristopher.knobel@usmc.mil

Capt Michael Flanagan
808 477-4997
michael.flanagan@usmc.mil

Information Protection
Command Security Manager
Brian Chun-Ming
808-477-8704
brian.chunming@usmc.mil

Imminent Threats
Call 9-1-1!